## AMENDMENTS TO THE CLAIMS

**Claims 1-42 (Cancelled)**

**Claim 43 (New)** A recording apparatus for recording encrypted content onto a recording medium having a read-only unrewritable area and a rewritable area to which data can be recorded and from which data can be read, the recording apparatus being one component of a digital work protection system including a plurality of reproduction apparatuses that each attempt to decrypt the encrypted content recorded onto the recording medium, the recording apparatus comprising:

a storing unit operable to store a piece of media key data that includes a plurality of encrypted media keys, each encrypted media key being generated (i) for a respective unrevoked reproduction apparatus of a plurality of unrevoked reproduction apparatuses and (ii) by encrypting a media key based on a device key assigned to the respective unrevoked reproduction apparatus;

an existence confirmation unit operable to confirm whether or not the piece of media key data exists on the recording medium, the confirmation being made when content is to be recorded onto the recording medium;

a content encrypting unit operable to encrypt the content, based on a content key, to generate the encrypted content, the content being a piece of digital data;

a key encrypting unit operable to generate an encrypted content key by encrypting the content key based on a media key obtained from the piece of media key data stored in the storage unit, the encrypted content key being generated when the existence confirmation unit confirms

that the piece of media key data does not exist on the recording medium; and

a writing unit operable to record the encrypted content, the encrypted content key, and the piece of media key data stored in the storage unit onto the rewritable area of the recording medium, the encrypted content, the encrypted content key, and the piece of media key data being recorded onto the rewritable area of the recording medium when the existence confirmation unit confirms that the piece of media key data does not exist on the recording medium.

**Claim 44 (New)** The recording apparatus of claim 43,

wherein, when the content is to be written onto the recording medium, the existence confirmation unit confirms whether or not (i) a piece of media key data having a generation that is the same as a generation of the piece of media key data stored in the storage unit, or (ii) a piece of media key data having a generation that is different from the generation of the piece of media key data stored in the storage unit, exists on the recording medium,

wherein the key encrypting unit encrypts the content key based on the media key obtained from the piece of media key data stored in the storage unit, to generate the encrypted content key, when the existence confirmation unit confirms that neither of (i) the piece of media key data having the generation that is the same as the generation of the piece of media key data stored in the storage unit and (ii) the piece of media key data having the generation that is different from the generation of the piece of media key data stored in the storage unit, exist on the recording medium, and

wherein the writing unit records the encrypted content, the encrypted content key and the piece of media key data stored in the storage unit to the rewritable area of the recording medium,

when the existence confirmation unit confirms that neither of (i) the piece of media key data having the generation that is the same as the generation of the piece of media key data stored in the storage unit and (ii) the piece of media key data having the generation that is different from the generation of the piece of media key data stored in the storage unit, exist on the recording medium.

**Claim 45 (New)** The recording apparatus of claim 44, wherein the existence confirmation unit confirms whether or not either of (i) the piece of media key data having the generation that is the same as the generation of the piece of media key data stored in the storage unit and (ii) the piece of media key data having the generation that is different from the generation of the piece of media key data stored in the storage unit, exist in the rewritable area of the recording medium.

**Claim 46 (New)** The recording apparatus of claim 44, further comprising:

a comparing unit operable to compare the piece of media key data recorded on the recording medium with the piece of media key data stored in the storage unit to judge which of the piece of the media key data stored in the recording medium and the piece of media key data stored in the storage unit is newer, the comparing unit performing the comparison when the existence confirmation unit confirms that either of (i) the piece of media key data having the generation that is the same as the generation of the piece of media key data stored in the storage unit and (ii) the piece of media key data having the generation that is different from the generation of the piece of media key data stored in the storage unit, exist on the recording medium; and

an updating unit operable to update the piece of media key data stored in the storage unit,

wherein, when the existence confirmation unit judges that either of (i) the piece of media key data having the generation that is the same as the generation of the piece of media key data stored in the storage unit and (ii) the piece of media key data having the generation that is different from the generation of the piece of media key data stored in the storage unit, exist on the recording medium and when the comparing unit judges that the piece of media key data recorded on the recording medium is newer, the updating unit reads the piece of media key data from the recording medium and updates the piece of media data stored in the storage unit with the piece of media key data read from the recording medium.

**Claim 47 (New)** The recording apparatus of claim 46,

wherein, when the existence confirmation unit confirms that either of (i) the piece of media key data having the generation that is the same as the generation of the piece of media key data stored in the storage unit and (ii) the piece of media key data having the generation that is different from the generation of the piece of media key data stored in the storage unit, exist on the recording medium and when the comparing unit judges that the piece of media key data recorded on the recording medium is older, the key encrypting unit further encrypts the content key based on the media key obtained from the piece of media key data stored in the storage unit, to generate the encrypted content key, and

wherein the writing unit further records the encrypted content key to the rewritable area of the recording medium.

**Claim 48 (New)** The recording apparatus of claim 47, further comprising:

a reading unit operable to read the encrypted content key from the rewritable area of the recording medium; and

a content key decrypting unit operable to decrypt the read encrypted content key based on the media key obtained from the piece of media key data recorded to the recording medium, to generate the content key, and

wherein the key encrypting unit further encrypts the content key generated by the content key decrypting unit, based on the media key obtained from the piece of media key data stored in the storage unit, to generate the encrypted content key, and

wherein the writing unit further records the encrypted content key to the rewritable area of the recording medium.

**Claim 49 (New)** The recording apparatus of claim 46,

wherein the piece of media key data stored in the storing unit includes a first piece of version information indicating the generation of the piece of media key data stored in the storing unit,

wherein the piece of media key data recorded on the recording medium includes a second piece of version information indicating the generation of the piece of media key data recorded on the recording medium, and

wherein the comparing unit judges which of, (i) the piece of media key data stored in the storing unit and (ii) the piece of media key data recorded on the recording medium, is newer by comparing the first piece of version information with the second piece of version information.

**Claim 50 (New)** The recording apparatus of claim 46,

wherein the piece of media key data stored in the storing unit includes a first piece of time information indicating a time at which the piece of media key data stored in the storing unit was generated,

wherein the piece of media key data recorded on the recording medium includes a second piece of time information indicating a time at which the piece of media key data recorded on the recording medium was generated, and

the comparing unit judges which of, (i) the piece of media key data stored in the storing unit and (ii) the piece of media key data recorded on the recording medium, is newer by comparing the first piece of time information with the second piece of time information.

**Claim 51 (New)** The recording apparatus of claim 44,

wherein the piece of media key data stored in the storing unit further includes a first data identifier that identifies the piece of media key data stored in the storing unit,

wherein the writing unit (i) records the first data identifier and the encrypted content to the rewritable area of the recording medium such that the first data identifier and the encrypted content are in correspondence, and (ii) records the piece of media key data including the first data identifier to the rewritable area of the recording medium.

**Claim 52 (New)** The recording apparatus of claim 51,

wherein the recording medium includes another piece of media key data including another set of encrypted media keys, each encrypted media key of the another set of encrypted

media keys being generated (i) for a respective unrevoked reproduction apparatus of a plurality of unrevoked reproduction apparatuses and (ii) by encrypting a media key based on a device key assigned to the respective unrevoked reproduction apparatus,

wherein the another piece of media key data includes a second data identifier that identifies the another piece of media key data recorded on the recording medium, and

wherein the recording apparatus further includes an assigning unit operable to assign the first data identifier, which is different from the second data identifier, to the piece of media key data stored in the storing unit.

**Claim 53 (New)** The recording apparatus of claim 51, further comprising:

a comparing unit operable to compare the piece of media key data stored in the storing unit with the piece of media key data recorded on the recording medium to judge which of the piece of media key data stored in the storing unit and the piece of media key data recorded on the recording medium is newer; and

an assigning unit operable to assign the first data identifier to the piece of media key data stored in the storing unit when the piece of media key data stored in the storing unit is judged to be newer.

**Claim 54 (New)** The recording apparatus of claim 53,

wherein the piece of media key data stored in the storing unit includes a first piece of time information indicating a time at which the piece of media key data stored in the storing unit was generated,

wherein the piece of media key data recorded on the recording medium includes a second piece of time information indicating a time at which the piece of media key data recorded on the recording medium was generated, and

wherein the comparing unit judges which of, (i) the piece of media key data stored in the storing unit and (ii) the piece of media key data recorded on the recording medium, is newer by comparing the first piece of time information with the second piece of time information.

**Claim 55 (New)** A recording method used by a recording apparatus operable to record encrypted content onto a recording medium having a read-only unrewritable area and a rewritable area to which data can be recorded and from which data can be read, the recording apparatus being one component of a digital work protection system including a plurality of reproduction apparatuses that each attempt to decrypt the encrypted content recorded onto the recording medium, the recording method comprising:

encrypting content, based on a content key, to generate the encrypted content, the content being a piece of digital data;

storing, in a storage unit, a piece of media key data including a plurality of encrypted media keys, each encrypted media key being generated (i) for a respective unrevoked reproduction apparatus of a plurality of unrevoked reproduction apparatuses and (ii) by encrypting a media key based on a device key assigned to the respective unrevoked reproduction apparatus;

confirming, when the content is to be recorded onto the recording medium, whether or not the piece of media key data exists on the recording medium;

generating an encrypted content key by encrypting the content key based on a media key obtained from the piece of media key data stored in the storage unit, the generating of the encrypted content key being performed when the confirming of whether or not the piece of media key data exists on the recording medium confirms that the piece of media key data does not exist on the recording medium; and

recording the encrypted content, the encrypted content key, and the piece of media key data stored in the storage unit onto the rewritable area of the recording medium, the recording being performed when the confirming of whether or not the piece of media key data exists on the recording medium confirms that the piece of media key data does not exist on the recording medium.

**Claim 56 (New)** A computer-readable recording medium having a program recorded thereon, the program for controlling a recording apparatus operable to record encrypted content onto a recording medium having a read-only unrewritable area and a rewritable area to which data can be recorded and from which data can be read, the recording apparatus being one component of a digital work protection system including a plurality of reproduction apparatuses that each attempt to decrypt the encrypted content recorded onto the recording medium, and the program causing the recording apparatus to execute a method comprising:

encrypting content, based on a content key, to generate the encrypted content, the content being a piece of digital data;

storing, in a storage unit, a piece of media key data including a plurality of encrypted media keys, each encrypted media key being generated (i) for a respective unrevoked

reproduction apparatus of a plurality of unrevoked reproduction apparatuses and (ii) by encrypting a media key based on a device key assigned to the respective unrevoked reproduction apparatus;

confirming, when the content is to be recorded onto the recording medium, whether or not the piece of media key data exists on the recording medium;

generating an encrypted content key by encrypting the content key based on a media key obtained from the piece of media key data stored in the storage unit, the generating of the encrypted content key being performed when the confirming of whether or not the piece of media key data exists on the recording medium confirms that the piece of media key data does not exist on the recording medium; and

recording the encrypted content, the encrypted content key, and the piece of media key data stored in the storage unit onto the rewritable area of the recording medium, the recording being performed when the confirming of whether or not the piece of media key data exists on the recording medium confirms that the piece of media key data does not exist on the recording medium.

**Claim 57 (New)** A computer-readable recording medium comprising:

a read-only unrewritable area; and

a rewritable area to which data can be recorded and from which data can be read,

wherein a medium inherent number that is inherent to the computer-readable recording medium is prestored in the unrewritable area,

wherein a piece of media key data, an encrypted content, and an encrypted content key

are recorded in the rewritable area,

wherein the piece of media key data includes a plurality of encrypted media keys, each encrypted media key being generated (i) for a respective unrevoked reproduction apparatus of a plurality of unrevoked reproduction apparatuses and (ii) by encrypting a media key based on a device key assigned to the respective unrevoked reproduction apparatus,

wherein the encrypted content is generated by encrypting content, based on a content key, to generate the encrypted content, the content being a piece of digital data, and

wherein the encrypted content key is generated by encrypting the content key based on the media key.

**Claim 58 (New)** A digital work protection system comprising:

a recording apparatus for recording encrypted content onto a recording medium having a read-only unrewritable area and a rewritable area to which data can be recorded and from which data can be read; and

a plurality of reproduction apparatuses, each reproduction apparatus being operable to attempt to decrypt the encrypted content recorded onto the recording medium,

wherein a piece of media key data and an encrypted content are recorded in the rewritable area of the recording medium,

wherein the piece of media key data includes a plurality of encrypted media keys, each encrypted media key being generated (i) for a respective unrevoked reproduction apparatus of a plurality of unrevoked reproduction apparatuses and (ii) by encrypting a media key based on a device key assigned to the respective unrevoked reproduction apparatus,

wherein the encrypted content is generated by encrypting content based on a content key, the content being a piece of digital data,

wherein the recording apparatus includes:

a content encrypting unit operable to encrypt the content, based on the content key, to generate the encrypted content;

a storing unit operable to store the piece of media key data;

an existence confirmation unit operable to confirm whether or not the piece of media key data exists on the recording medium;

a key encrypting unit operable to generate an encrypted content key by encrypting the content key based on a media key obtained from the piece of media key data stored in the storage unit, the encrypted content key being generated when the existence confirmation unit confirms that the piece of media key data does not exist on the recording medium; and

a writing unit operable to record the encrypted content, the encrypted content key, and the piece of media key data stored in the storage unit onto the rewritable area of the recording medium, the encrypted content, the encrypted content key, and the piece of media key data being recorded onto the rewritable area of the recording medium when the existence confirmation unit confirms that the piece of media key data does not exist on the recording medium, and

wherein each reproduction apparatuses includes:

a reading unit operable to read the piece of media key data recorded onto the rewritable area of the recording medium or read part of the piece of media key data recorded onto the rewritable area of the recording medium;

a decrypting unit operable to decrypt an encrypted media key from the piece or part of media key data read by the reading unit, the decrypting unit decrypting the encrypted media key using the device key assigned to the reproduction apparatus, to generate a decryption media key; and

a decrypting unit operable to read the encrypted content from the recording medium and decrypt the read encrypted content based on the generated decryption media key, to generate decrypted content.